ICS 35.240.40
CCS A 11

JR

中华人民共和国金融行业标准

JR/T 0234—2021

数字函证金融应用安全规范

Security specification for financial digital confirmation

2021－09－27 发布　　2021－09－27 实施

中国人民银行　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国人民银行提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

数字函证金融应用安全规范

1 范围

本文件规定了金融机构数字函证业务系统和数字函证基础设施的安全技术要求、安全管理要求、业务运营安全要求等。

本文件适用于开展数字函证业务的金融机构以及数字函证基础设施建设运营单位。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 39786 信息安全技术 信息系统密码应用基本要求

JR/T 0068 网上银行系统信息安全通用规范

JR/T 0071 金融行业网络安全等级保护实施指引

JR/T 0118 金融电子认证规范

JR/T 0184 金融分布式账本技术安全规范

JR/T 0185 商业银行应用程序接口安全管理规范

JR/T 0193 区块链技术金融应用 评估规则

JR/T 0197 金融数据安全 数据安全分级指南

JR/T 0223 金融数据安全 数据生命周期安全规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

函证 confirmation

会计师事务所等在取得被审计单位授权后，直接向金融机构发出询证函，金融机构针对所收到的询证函，查询、核对相关信息并直接提供书面回函的过程。

3.2

数字函证 digital confirmation

会计师事务所等在取得被审计单位授权后，应用数字化手段向金融机构发出询证函，金融机构应用数字化手段受理会计师事务所等数字函证请求，提供符合函证数据标准的数字回函的过程。

3.3

数字函证联系 digital confirmation correspondence

指会计师事务所或被审计单位与金融机构的数字函证联系，可通过金融机构数字函证业务系统直接连接或通过数字函证基础设施间接连接方式实现。

3.4

数字函证基础设施 digital confirmation infrastructure

由独立第三方提供的支持会计师事务所、被审计单位与金融机构实现数字函证联系的公共基础设施，符合集约化、规范化、数字化的要求。

3.5

会计师事务所 accounting firm

经被审计单位授权后，发起数字函证请求的具有合法执业资质的机构。

3.6

被审计单位 auditee

会计师事务所的审计对象。

注：被审计单位授权会计师事务所向银行业金融机构等发起询证函并接收函证。

3.7

金融机构数字函证业务系统 financial institutions digital confirmation system

可汇总提供被审计单位在金融机构的所有函证业务信息的集中处理系统。

3.8

证书 certificate

关于实体的一种数据，该数据由认证机构的私钥或秘密密钥签发，并无法伪造。

[来源：GB/T 25069，2.2.2.218]

3.9

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

[来源：GB/T 25069，2.2.2.176]

3.10

访问控制 access control

一种保证数据处理系统的资源只能由被授权主体按授权方式进行访问的手段。

[来源：GB/T 25069，2.2.1.42]

3.11

智能密码钥匙 cryptographic smart token

提供密码运算、密钥管理等密码服务的终端密码设备，一般使用USB、蓝牙、音频、SD等接口形态。

[来源：JR/T 0068，3.7]

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

App_ID：应用唯一标识（Application unique ID）

App_Secret：应用鉴别密文（Application Secret）

CA：证书颁发机构（Certificate Authority）

LEI：全球法人识别编码（Legal Entity Identifier）

SD：安全数码（Secure Digital）

SQL：结构化查询语言（Structured Query Language）

TEE：可信执行环境（Trusted Execution Environment）

USB：通用串行总线（Universal Serial Bus）

VPN：虚拟专用网络（Virtual Private Network）

5 数字函证业务

5.1 业务概述

数字函证联系模式可以分为数字函证基础设施间接连接模式和金融机构数字函证业务系统直接连接模式，数字函证业务模式如图所示。

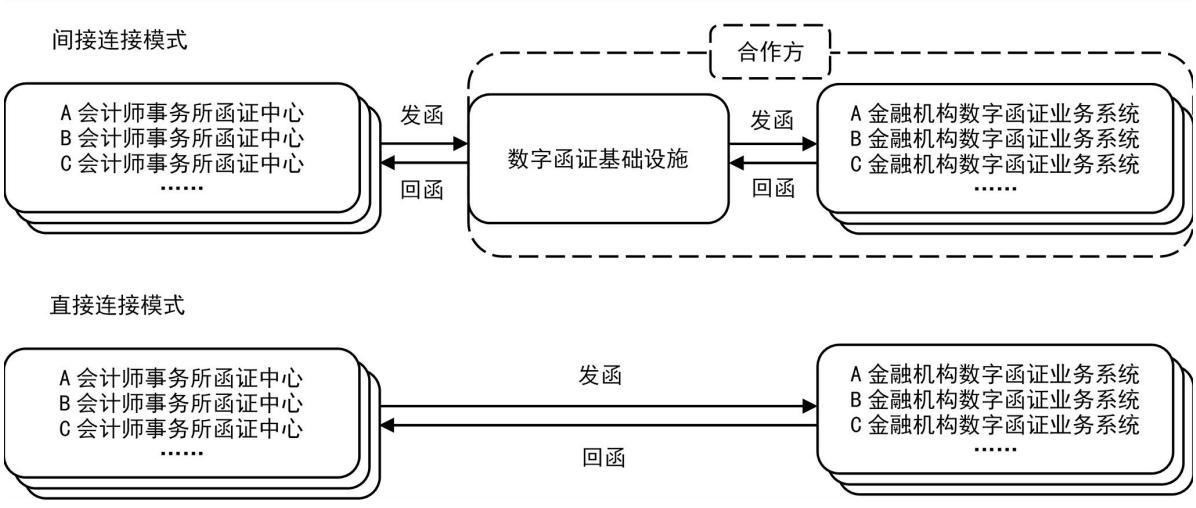

图 数字函证业务模式

在间接连接模式下，数字函证基础设施运营单位与金融机构互为合作方，会计师事务所等为被服务方。该模式下，会计师事务所通过数字函证基础设施发送函证至金融机构，金融机构受理被审计单位授权的函证并回函，会计师事务所通过数字函证基础设施获取金融机构的回函。数字函证基础设施应符合集约化、规范化、数字化的要求，应在数据安全防护、控制权设计、运营模式等方面采取必要的安全措施。数字函证基础设施应具有网络安全等级保护三级认证。通过数字函证基础设施传输的函证数据应由会计师事务所或金融机构加密，数字函证基础设施应无法对函证数据进行解密。

在直接连接模式下，金融机构通过自建数字函证业务系统直接为会计师事务所提供数字函证服务。该模式下，会计师事务所发送函证至金融机构数字函证业务系统，金融机构通过数字函证业务系统受理被审计单位授权的函证并回函，会计师事务所通过金融机构数字函证业务系统获取回函。

数字函证基础设施运营单位和金融机构应支持配合监管部门开展函证业务监管工作。监管部门在保证函证数据安全、数字函证业务合规的前提下，对数字函证业务进行监管。数字函证基础设施运营单位及合作单位应获得监管部门的授权或认可。

5.2 系统构成

数字函证基础设施和金融机构数字函证业务系统主要由接入端、通信网络、服务端组成。对于数字函证基础设施间接连接模式，会计师事务所和金融机构是接入端，数字函证基础设施是服务端；对于金融机构数字函证业务系统直接连接模式，会计师事务所等是接入端，金融机构是服务端。

数字函证基础设施和金融机构数字函证业务系统在设计、开发、部署和运营过程中，应审慎评估业务、网络安全、数据安全及外包等风险，并针对各类风险进行有效防护。

数字函证基础设施之间应支持互联互通，为金融机构、会计师事务所等开展数字函证业务和监管部门统筹监管提供便利。

5.2.1 接入端

数字函证基础设施和金融机构数字函证业务系统通过网页（Web）应用或API对接方式提供发函、回函、流程管理等服务，会计师事务所可根据实际情况进行适配。

5.2.2 通信网络

数字函证基础设施和金融机构数字函证业务系统通过互联网或专用网络向会计师事务所提供数字函证联系服务，应从网络安全层面采取措施有效应对安全风险。

5.2.3 服务端

数字函证基础设施和金融机构数字函证业务系统应充分利用物理与环境安全、网络与通信安全、设备与计算安全、应用与数据安全等领域的防护手段，综合使用密码学、安全协议、TEE等技术保证函证数据的机密性、完整性和不可抵赖性。

6 数字函证安全要求

6.1 安全要求概述

数字函证基础设施和金融机构数字函证业务系统应遵照国家和金融行业相关安全标准进行建设，并遵循本文件关于安全技术、安全管理和安全运营的相关要求。

6.2 安全技术要求

6.2.1 通用安全

数字函证基础设施和金融机构数字函证业务系统的物理与环境安全、网络与通信安全、设备与计算安全、应用与数据安全应遵循JR/T 0071中关于系统第三级安全保护的要求。

6.2.2 密码安全

数字函证基础设施和金融机构数字函证业务系统使用的密码算法、密码产品以及密码服务应遵循国家密码管理部门相关要求，并遵循GB/T 39786的要求。

6.2.3 数字函证业务安全

6.2.3.1 接入端安全

数字函证基础设施和金融机构数字函证业务系统使用的密码硬件设备（如智能密码钥匙、加密卡等）及安全认证设备应符合行业主管部门和国家密码管理部门的要求，同时应满足JR/T 0068中6.2.2的要求。

6.2.3.2 身份认证

对使用数字函证基础设施和金融机构数字函证业务系统的用户（以下简称用户）进行身份认证时，遵循如下要求：

a) 对通过API方式对接的用户进行身份认证时，应遵循如下要求：
   1) 使用的验证要素包括 App_ID 和 App_Secret，App_ID 和数字证书，App_ID 和公私钥对，或上述三对要素的组合。
   2) 使用包含数字证书或公私钥对的方式进行双向身份认证。
   3) 建立 IP 地址白名单，仅允许在白名单内的 IP 地址进行网络通信并访问函证业务接口，应支持 IP 地址白名单动态更新。
b) 对通过Web方式对接的用户进行身份认证时，应遵循如下要求：
   1) 按照审慎原则，采取有效、可靠的身份认证手段，保证数据安全。
   2) 采取验证强度与数据敏感度相匹配的技术措施，提高安全性。高风险业务应在下列三类要素中选用两组及以上进行验证：一是用户知悉的要素，如静态密码等；二是仅用户本人持有并特有的，不可复制或者不可重复利用的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等；三是用户本人生物特征要素，如指纹、虹膜等。要素应相互独立，部分要素的损坏或者泄露不应导致其他要素损坏或者泄露。
   3) 提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。
   4) 对于系统自动分配或者预设的强度较弱的初始密码，应强制用户首次登录时修改初始密码，并要求用户设置具有一定密码强度的密码。应要求用户定期更换密码，修改密码时，新设定的密码不应与旧密码相同。应支持用户锁定策略。采用一次性密码作为验证要素的，应将一次性密码有效期严格限制在最短的必要时间内。
   5) 仅支持同一用户单点登录，同一用户多点登录仅保留最新会话，并向用户发送系统消息和短信进行提醒。
   6) 具备良好的可扩展性，可快速实现对动态口令、生物识别等其他认证方式的支持。

6.2.3.3 通信链路安全

数字函证基础设施和金融机构数字函证业务系统通信链路的建立过程和传输过程应使用密码技术进行保护，并遵循如下要求：

a) 应在客户端程序与服务器之间建立安全的信息传输通道，采用安全稳定的安全协议并及时更新至最新版本，不可使用存在重大安全隐患版本的协议。
b) 每次会话宜采取独立不同密钥对业务数据进行加密处理，防止业务数据被窃取或者被篡改。
c) 应使用密码技术和安全通信协议保证传输数据的机密性和完整性，且密码算法应符合国家密码管理部门的相关要求。
d) 通过公开网络进行数据传输时，应通过密钥对、证书等密码技术手段进行双向认证。

e) 可采用隧道技术、加解密技术、密钥管理技术、身份认证技术在系统与用户之间构建虚拟专用网络（VPN）,拥有适当权限的用户才能通过远程访问建立连接。

6.2.3.4 Web 应用安全

数字函证基础设施和金融机构数字函证业务系统在Web应用安全方面遵循如下要求：

a) 应能够防范函证敏感信息泄露。
b) 应能够防范SQL注入攻击。
c) 应能够防范跨站脚本攻击。
d) 应对Web页面提供的链接和内容进行控制，定期检查外部链接和引用内容的安全性。
e) 应采取网站页面防篡改措施，应具备对Web后门进行检测和报警的能力。
f) 应加强对开源及商业应用系统或组件的安全管理，进行安全评估并及时修复安全漏洞。
g) 应对文件的上传和下载进行访问控制，避免攻击者执行恶意文件或发起未授权访问。
h) 应采取有效措施防范针对服务器端应用层的拒绝服务攻击。

6.2.3.5 接口安全

数字函证基础设施提供核心的发函、回函、流程管理等接口，包括但不限于：发函接口、函证状态查询接口、发函获取接口、发函驳回接口、回函接口、回函获取接口、异常处理接口。金融机构数字函证业务系统提供核心的发函、回函、流程管理等接口，包括但不限于：发函接口、函证状态查询接口、发函获取接口、发函驳回接口、回函接口、回函获取接口、异常处理接口。会计师事务所、金融机构可调用接口完成相应的函证业务。

数字函证基础设施和金融机构数字函证业务系统接口遵循如下要求：

a) 应具有接口说明材料，对接口的功能、格式、方法、参数、返回值、使用方式等进行详细说明，接口文档中应提供完整的错误码和含义。
b) 应明确用户能够调用的接口列表，并进行权限控制。
c) 应设计良好的接口，隐藏数字函证基础设施和金融机构数字函证业务系统的实现细节，提供简洁的调用方法。
d) 应具备良好的扩展性和兼容性。
e) 应保证内部各模块之间接口交互的安全性和完整性。
f) 应仅支持会计师事务所等调用数字函证基础设施发函相关接口，包括：发函接口、函证状态查询接口、回函获取接口等。
g) 应仅支持金融机构调用数字函证基础设施回函相关接口，包括：发函获取接口、回函接口、发函驳回接口等。
h) 对以API方式对接的用户，数字函证基础设施或金融机构数字函证业务系统和用户系统应在安全通信环境下使用数字证书等方式进行认证，并保证接口的完整性、机密性和不可抵赖性。
i) 接口设计应符合JR/T 0185的要求。

6.2.3.6 被审计单位授权

金融机构回函前应按照相关监管要求获得被审计单位授权，授权遵循如下要求：

a) 被审计单位的授权方式可使用“企业网银账户名+密码”和企业网银智能密码钥匙的双因子认证方式。使用其他授权方式时，被审计单位使用的授权方式安全性不宜低于上述方式，其中至少一种认证要素应使用密码硬件设备。
b) 应明确被审计单位的授权范围、授权时间以及被调用记录等，方便被审计单位查询核实。

6.2.4 函证数据安全

6.2.4.1 数据分级保护

数字函证基础设施和金融机构数字函证业务系统在数据分级保护方面遵循如下要求：

a) 函证数据应根据JR/T 0197要求进行分级分类保护，相关函证数据至少定为三级。
b) 应参照JR/T 0071中对重要业务数据的要求采取相应的安全保护措施。
c) 应参照JR/T 0223中对数据生命周期保护的安全要求，以数据分级为基础，建立覆盖数据生命周期全过程的安全防护体系，并通过建立健全数据安全组织架构和明确信息系统运维环节中的数据安全需求，全面保障金融机构数据安全。
d) 金融机构对函证数据进行数字化处理时，应遵循金融行业信息安全标准要求，实现函证数据的机密性、完整性和不可抵赖性。
e) 涉及国家秘密的函证数据，应依据国家有关法律法规执行，不在本文件规定的范围之内。

6.2.4.2 数据访问控制

数字函证基础设施和金融机构数字函证业务系统数据访问控制遵循如下要求：

a) 应确保金融机构和会计师事务所仅能获取与本单位相关的函证数据。
b) 应支持监管部门依法获取相应的函证数据。
c) 通过数字函证基础设施传输的函证数据应由会计师事务所或金融机构加密，数字函证基础设施应无法对函证数据进行解密。
d) 应支持实施授权和制衡机制，实现管理权限与操作权限分离，使金融机构和会计师事务所在确保安全的前提下，根据用户角色访问对应的函证数据。
e) 应详细记录系统操作日志，加强对回函流程信息的记录管理，日志文件应至少妥善保存三个月。

6.2.4.3 数据传输安全

数字函证基础设施和金融机构数字函证业务系统应采取数据传输加密、身份认证等技术措施加强数据传输过程的安全防护。根据金融数据分级及数据输出相关要求（如JR/T 0197、JR/T 0223等），函证数据宜采用专线确保传输通道的安全，业务量少的中小金融机构向数字函证基础设施传输数据时，可选择采用VPN等技术确保数据传输的安全性。

6.2.4.4 数据不可抵赖性

数字函证基础设施和金融机构数字函证业务系统应通过数字签名技术保证函证数据的不可抵赖性，数字签名技术遵循如下要求：

a) 应支持发函数据由会计师事务所进行数字签名，金融机构应能够对发函的数字签名进行校验。
b) 应支持回函数据由金融机构进行数字签名，会计师事务所应能够对回函的数字签名进行校验。
c) 应支持验证用户数字证书的有效性。
d) 应支持验证数字签名的有效性。
e) 应支持验证产生签名的数字证书与用户的关联关系。
f) 使用第三方CA或者自建电子认证服务的，数字证书及生成电子签名的过程应符合《中华人民共和国电子签名法》以及《金融电子认证规范》的要求。

6.2.5 区块链应用安全

数字函证基础设施和金融机构数字函证业务系统如采用区块链技术，应严格遵守区块链信息服务管理规定和金融监管要求，并结合实际情况，在遵循 JR/T 0184、JR/T 0193 等金融相关标准和规定的基

础上，开展区块链技术应用备案工作，建立健全区块链技术应用风险防控机制，定期开展外部安全评估。

6.3 安全管理要求

数字函证基础设施的安全管理应参照JR/T 0071中8.1.5、8.1.6、8.1.7、8.1.8、8.1.9、8.1.10的规定执行。

金融机构数字函证业务系统的安全管理应根据系统的定级级别，参照JR/T 0071规范中对应等级的安全管理规定执行。应有效实施授权和制衡机制，通过内部审计、内控评价等方式对回函工作进行内部监督和问责。系统无法自动填制信息或校验回函的金融机构，应当有效落实人工复核要求，实现不相容职责的分离。完善对函证回函工作的内部控制，对回函信息的真实性、准确性负责。

6.4 安全运营要求

6.4.1 合作及服务管理

数字函证基础设施运营单位与金融机构在数字函证有关合作及服务方面应加强管理，并遵循如下要求：

a) 数字函证基础设施运营单位与金融机构合作开展函证业务，为会计师事务所等提供数字函证服务时，遵循如下安全要求：
   1) 应建立与金融机构合作、为会计师事务所等服务的风险管理机制，明确技术、业务等相关部门职责，制定风险管理制度，建立安全技术标准，规范系统接入，并加强对业务开展情况的动态管理。
   2) 应与金融机构、会计师事务所等签订数字函证基础设施使用协议，明确数字函证基础设施与金融机构、会计师事务所等基于数字函证基础设施开展函证业务的权利、义务和违约责任。
   3) 应要求金融机构、会计师事务所等提供本机构相关材料或信息，如LEI等。应对金融机构、会计师事务所等提交的申请材料的真实性、完整性和合规性进行审核，对审核通过的金融机构、会计师事务所等创建用户账号，建立账号与智能密码钥匙的关联关系，并发放智能密码钥匙。
   4) 应对金融机构、会计师事务所等智能密码钥匙的生命周期进行管理。
   5) 应采取将安全设备序列号与用户信息进行绑定等措施，如智能密码钥匙丢失，金融机构、会计师事务所等应提交相关材料重新办理，并解除原有智能密码钥匙和用户的绑定关系。
   6) 智能密码钥匙在暂停、终止、挂失或注销后，如需要恢复、解除挂失，应要求金融机构、会计师事务所等提交本机构申请材料，并重新审核申请材料的真实性、完整性和合规性。
b) 金融机构通过数字函证基础设施或自建数字函证业务系统为会计师事务所等提供数字函证服务时，遵循如下安全要求：
   1) 应建立与数字函证基础设施运营单位合作、为会计师事务所等服务的风险管理机制，明确技术、业务等相关部门职责，制定风险管理制度，建立安全技术标准，规范系统接入，并加强对业务开展情况的动态管理。
   2) 应与会计师事务所等签订金融机构数字函证业务系统使用协议，明确金融机构与会计师事务所等基于金融机构数字函证业务系统开展函证业务的权利、义务和违约责任。
   3) 应要求会计师事务所等提供本机构相关材料或信息，如LEI等。应对会计师事务所等提交的申请材料的真实性、完整性和合规性进行审核，对审核通过的会计师事务所创建用户账号，建立安全管理机制。

6.4.2 业务外包

数字函证基础设施运营单位和金融机构应具备金融机构数字函证业务系统的自主运维能力，不应将核心业务外包。将数字函证业务系统非核心业务外包的金融机构须按照中国人民银行、中国银行保险监督管理委员会、中国证券监督管理委员会等监管部门关于信息科技外包的管理要求进行管理。数字函证基础设施应参照金融行业基础设施有关要求进行管理。

6.4.3 培训与权益保护

数字函证基础设施和金融机构数字函证业务系统在培训与权益保护方面遵循如下要求：

a) 应切实加强用户培训和风险提示，向用户详细解释数字函证基础设施和金融机构数字函证业务系统的业务流程和安全控制措施，在新功能推出、相关业务（操作）流程变更、安全控制措施变化时，应及时告知用户。
b) 对API接入方式的用户，应提供完整的接口使用说明和测试环境，进行技术对接专项培训，并保证测试通过后再切换到生产环境开展函证业务。
c) 对Web接入方式的用户，应提供详细的业务操作手册。
d) 应制定用户隐私保护政策。
e) 针对服务内容、协议等重大调整，可能影响服务的系统重要升级或变更等重大事项，应提前通知用户。

7 互联互通安全要求

7.1 通用安全

数字函证基础设施之间应支持互联互通，在通用安全方面遵循如下要求：

a) 应具有相同的网络安全保护等级，以保证不同基础设施的用户得到与互联互通前相同的保护级别。
b) 使用第三方CA的电子认证服务时，数字证书及生成电子签名的过程应符合《中华人民共和国电子签名法》以及《金融电子认证规范》的要求。第三方CA的电子认证服务应满足数字函证基础设施的互联互通需求。
c) 对接系统之间的接口应遵循6.2.3.5的安全要求。
d) 对接系统的安全管理应遵循6.3的安全要求。
e) 对接系统的基础设施运营应遵循6.4的安全要求。
f) 合理设计管理机制及协议，跨基础设施函证业务应得到不同基础设施用户的授权确认。

7.2 接入网络安全

7.2.1 通讯方式

数字函证基础设施之间互联互通时，应符合GB/T 22239中8.1.2的规定。

7.2.2 生产网络安全

数字函证基础设施之间互联互通时，生产网络安全遵循如下要求：

a) 生产网络应与不涉及数字函证业务的其他网络逻辑隔离。
b) 生产网络接入互联网前应严格审批。
c) 应建立对所有路由配置和防火墙策略的批准、测试和变更的正式流程，路由配置和防火墙策略在每次变更后应及时归档。

d) 应定期对路由配置和防火墙策略进行检查，对路由器和防火墙的事件日志、入侵检测设备的告警事件进行分析和处理。
e) 应对登录网络及网络安全设备的用户进行身份鉴别，严格控制修改网络及网络安全设备配置账号的操作。
f) 应及时进行网络及网络安全设备的补丁安装和版本升级，及时更新入侵检测系统的防护知识库。
g) 定期或者在网络发生重大变更时，应对安全控制措施、网络连接和限制措施进行渗透性测试或漏洞扫描，对网络及网络安全设备系统设置、补丁配置和已知的漏洞进行检查，生产网络用户不应私自连接到外部网络，外部访问不应非授权进入生产网络。
h) 应在网络边界处部署防入侵检测设备，监视可能的攻击行为，记录入侵事件，并报警正在发生的入侵事件。
i) 应采取物理隔离、划分虚拟局域网、主机路由等方式分割不同的用户和信息系统，阻止非授权用户对内部网络中敏感数据的访问。
j) 应定期开展对网络和网络安全设备的内部或外部审计，验证其配置或策略与入网机构安全要求的符合程度。
k) 应在网络边界及核心业务网段处对恶意代码进行检测或清除。

7.2.3 数据交换安全

数字函证基础设施之间互联互通，在涉及用户信息的传输交换时，应充分重视信息转移或交换过程中的安全风险，并遵循如下要求：

a) 在数据传输前，应开展用户信息安全影响评估，并依据评估结果采取有效措施保护用户信息主体权益。
b) 在数据传输前，应开展用户信息接收方安全保障能力评估，并签署数据保护责任承诺。
c) 应部署防信息泄漏监控工具，监控及报告用户信息的违规外发行为。
d) 应部署流量监控技术措施，对转移或交换的用户信息进行监控和审计。
e) 应定期检查或评估用户信息导出通道的安全性和可靠性。
f) 应执行严格的审核程序，并准确记录和保存用户信息数据传输的情况。记录内容包括但不限于日期、规模、目的、范围，以及数据接收方基本情况与使用意图，并应确保对传输的用户信息及其过程可追溯。
g) 在用户信息转移过程中，应采取有效的技术防护措施，防范被除信息发送方与接收方之外的其他个人、组织和机构截获和利用。

7.3 区块链应用安全

采用区块链技术的数字函证基础设施之间互联互通时，区块链应用应符合JR/T 0184和JR/T 0193的规定，并遵循如下要求：

a) 应在数字函证基础设施之间建立安全传输通道，保证数据传输的完整性与不可篡改性。
b) 应采用密码技术保障数字函证基础设施之间通信过程中敏感信息字段或整个报文的安全性。
c) 应确保信息在存储、传输过程中不被非授权用户读取和篡改。

参考文献

[1] 《财政部 人民银行 国务院国资委 银保监会 证监会 国家档案局 国家标准化管理委员会关于推进会计师事务所函证数字化相关工作的指导意见》（财会〔2020〕13号）.2020-09-07

[2] 《财政部 银保监会关于进一步规范银行函证及回函工作的通知》（财会〔2020〕12号）.2020-08-10

[3] 《财政部办公厅 银保监会办公厅关于印发银行函证及回函工作操作指引的通知》（财办会〔2020〕21号）.2020-08-10

[4] 《中国人民银行关于发布金融行业标准推动区块链技术规范应用的通知》（银发〔2020〕162号）.2020-07-13